SPYWARE

Just when you thought you were Web savvy, one more privacy, security, and functionality issue crops up — spyware. Installed on your computer without your consent, spyware software monitors or controls your computer use. It may be used to send you pop-up ads, redirect your computer to websites, monitor your Internet surfing, or record your keystrokes, which, in turn, could lead to identity theft.

Many experienced Web users have learned how to recognize spyware, avoid it, and delete it. According to OnGuard Online, all computer users should take preventive steps to avoid spyware, get wise to the signs that it has been installed on their machines, and then take the appropriate steps to delete it.

The clues that spyware is on a computer include:

- Barrage of pop-ups
- Hijacked browser — that is, a browser that takes you to sites other than those you type into the address box
- A sudden or repeated change in your computer’s Internet home page
- New and unexpected toolbars
- New and unexpected icons on the system tray at the bottom of your computer screen or on your desktop
- Keys that don’t work (for example, the “Tab” key that might not work when you try to move to the next field in a Web form)
- Random error messages
- Sluggish or downright slow performance when opening programs or saving files

The good news is that consumers can take steps to lower their risk of spyware infections. Indeed, OnGuard Online suggests that you:

Update your operating system and Web browser software. Your operating system (like Windows or Linux) may offer free software “patches” to close holes in the system that spyware could exploit. Set your operating system and security software to update automatically to be sure you have the latest protections.

SPYWARE

Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly. You can download this software from ISPs or software companies or buy it in retail stores. Look for anti-virus and anti-spyware software that removes or quarantines viruses and that updates automatically on a daily basis.

Download free software only from sites you know and trust. It can be appealing to download free games, file-sharing programs, or customized toolbars. Be aware, however, that some of these free software applications bundle other software, including spyware. If you share a computer with kids, talk with them about safe computing.

Don't install any software without knowing exactly what it is. Take the time to read the end-user license agreement (EULA) before downloading any software. If the EULA is hard to find — or difficult to understand — think twice about installing the software.

Minimize "drive-by" downloads. Make sure your browser security setting is high enough to detect unauthorized downloads, for example, at least the "Medium" setting for Internet Explorer.

Don't click on any links within pop-ups. If you do, you may install spyware on your computer. Instead, close pop-up windows by clicking on the "X" icon in the title bar.

Don't click on links in spam or pop-ups that claim to offer anti-spyware software. Some software offered in spam or pop-ups actually *installs* spyware. In fact, ads that claim to have scanned your computer and detected malware are a tactic scammers have used to spread malware, so resist the urge to respond to or click on those messages.

Install a personal firewall to stop uninvited users from accessing your computer. A firewall blocks unauthorized access to your computer and will alert you if spyware already on your computer is sending information out.

Back up your data. Whether it's text files or photos that are important to you, back up any data that you'd want to keep in case of a computer crash. Do this as regularly as you update your security software.

SPYWARE

If you think your computer might have spyware on it, immediately stop shopping, banking, or doing any other online activity that involves user names, passwords, or other sensitive information. Confirm that your security software is active and current and run it to scan your computer for viruses and spyware, deleting anything the program identifies as a problem. Visit "Minimizing the Effects of Malware" for more detailed tips.

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

February 2008